



SIMPLILEARN

NALANDA 53/1 C, Manoj Arcade, 24th Main Rd, Sector 2, HSR Layout, Bengaluru - 560102, Karnataka, India. 1800-212-7688

Project

Conduct VAPT on a bank called "Altoro Mutual."

Submitted by Koushik Panda

Instructor

Baba Shaheer

Program

Professional Certificate Program in Cybersecurity- Red Team

Course

PCP CS: Penetration Testing



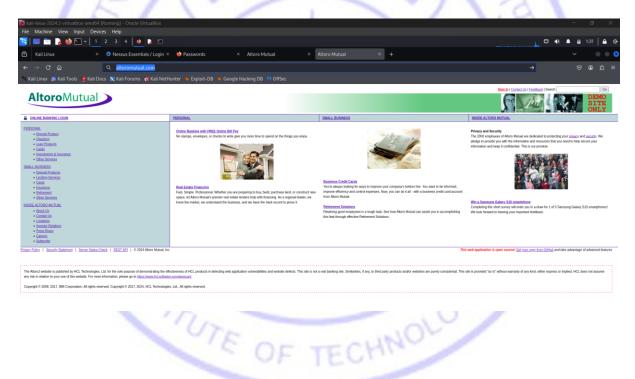
Task (Activities):

In this project, you will be testing the following vulnerabilities:

- Cross Site Scripting (XSS) Vulnerability
- SQL Injection
- Brute Force Attack
- Access Control Vulnerability
- HTML Injection



Victim Website - Altoro Mutual





Attacker machine (Kali Linux) – 10.10.10.4

```
(root⊕ kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.4 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::eb79:1188:21c0:6c37 prefixlen 64 scopeid 0×20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 106261 bytes 135617148 (129.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33374 bytes 4381383 (4.1 MiB)
    TX errors 0 dropped 8 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0×10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 14818 bytes 8119064 (7.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14818 bytes 8119064 (7.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ping Website – Altoro Mutual's IP (65.61.137.117)

```
ping altoromutual.com
PING altoromutual.com (65.61.137.117) 56(84) bytes of data.
64 bytes from 65.61.137.117: icmp_seq=1 ttl=243 time=310 ms
64 bytes from 65.61.137.117: icmp_seq=2 ttl=243 time=309 ms
64 bytes from 65.61.137.117: icmp_seq=3 ttl=243 time=309 ms
64 bytes from 65.61.137.117: icmp_seq=4 ttl=243 time=308 ms
^Z
zsh: suspended ping altoromutual.com
```



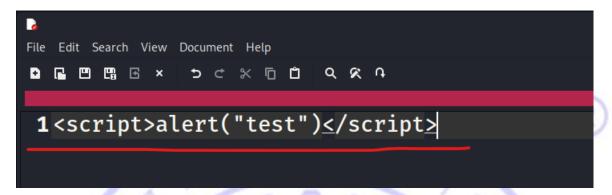
Scanning Website through Nikto and Nmap

```
nikto -h altoromutual.com
 - Nikto v2.5.0
                      65.61.137.117
+ Target IP:
                      altoromutual.com
+ Target Hostname:
+ Target Port:
+ Start Time:
                      2024-11-04 08:15:10 (GMT-5)
+ Server: Apache-Covote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to th
e MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ 7981 requests: 1 error(s) and 6 item(s) reported on remote host
+ End Time:
                      2024-11-04 09:07:20 (GMT-5) (3130 seconds)
+ 1 host(s) tested
```

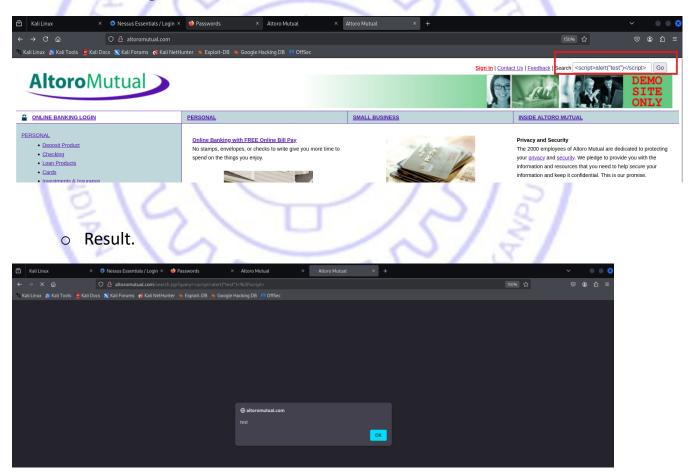
```
File Actions Edit View Help
 root@kali: ~ × root@kali: ~ × root@kali: ~ ×
    nmap -A -T5 65.61.137.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 08:27 EST
Nmap scan report for 65.61.137.117
Host is up (0.0025s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: NOTIMP)
80/tcp open http Apache Tomcat/Coyote JSP engin
                         Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Altoro Mutual
|_http-server-header: Apache-Coyote/1.1
443/tcp open ssl/http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
 _ssl-date: 2024-11-04T13:28:36+00:00; +3s from scanner time.
  ssl-cert: Subject: commonName=demo.testfire.net
 Subject Alternative Name: DNS:demo.testfire.net, DNS:altoromutual.com
  Not valid before: 2024-06-03T00:00:00
  _Not valid after: 2025-07-04T23:59:59
 |_http-title: Altoro Mutual
8080/tcp open http
                         Apache Tomcat/Coyote JSP engine 1.1
 |_http-server-header: Apache-Coyote/1.1
 |_http-title: Altoro Mutual
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-b
in/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=11/4%Time=6728CBE6%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|webcam|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (92%), Garmin embedded (89%), 2N embedded (88%), FireBrick embedded (85%), NodeMCU embedded (85%),
lwIP 1.4.X (85%), Philips embedded (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/h:firebrick:fb2700 cpe:/o:nodemcu:nodemcu cpe:/a:lwip_project:l
wip cpe:/h:philips:hue_bridge cpe:/a:lwip_project:lwip:1.4
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (92%), Garmin Virb Elite action camera (89%), 2N Helios IP VoIP doorbell (88%), FireBrick F
```



- First Task Cross Site Scripting (XSS) Vulnerability
 - Script –



Executing in the search area.

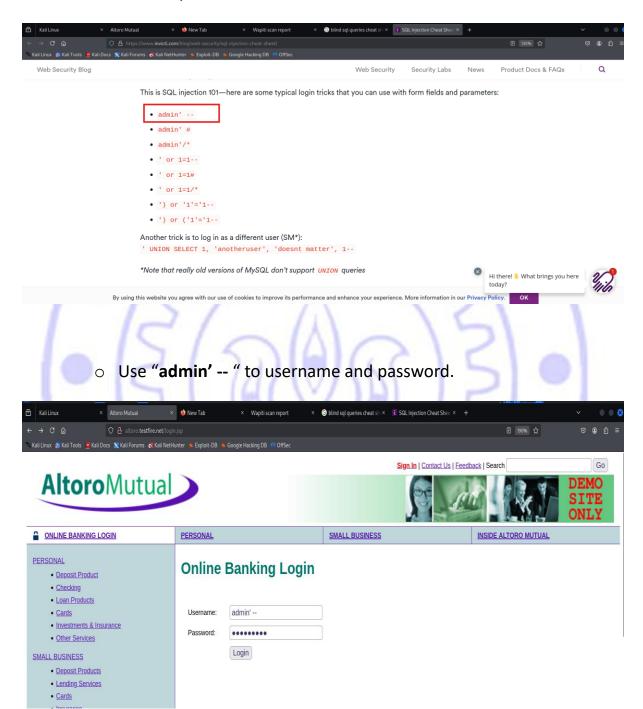


The Cross Site Scripting (XSS) attack is successful.



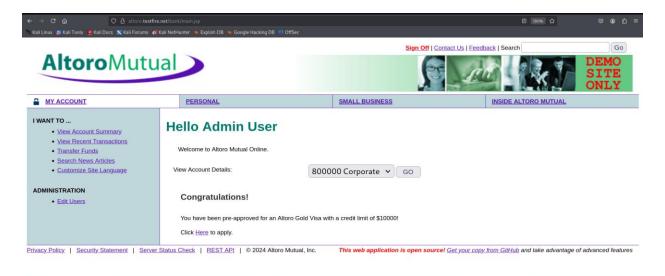
• Second Task: - SQL Injection

Blind SQL Attack.





o Result -



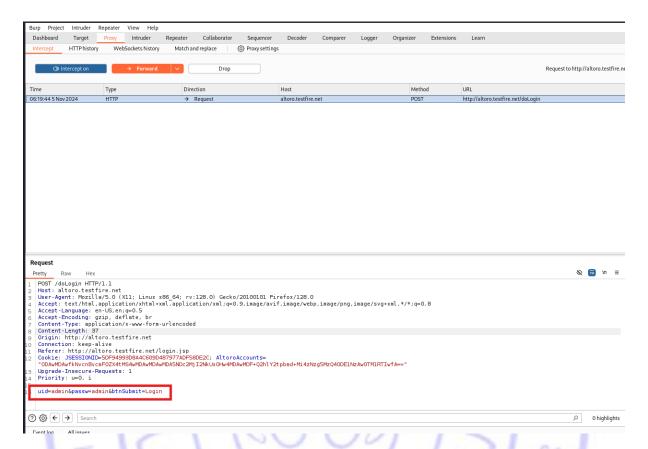
SQL Injection successful as login as an admin.

- Third Task: Brute Force Attack
 - Setting proxy in Firefox Browser.

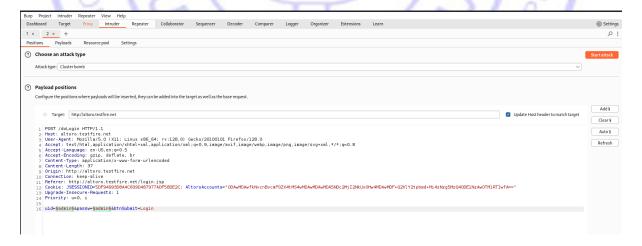




 Use Burpsuite tool for this attack, and this tool intercepts login credentials and now start the attack.

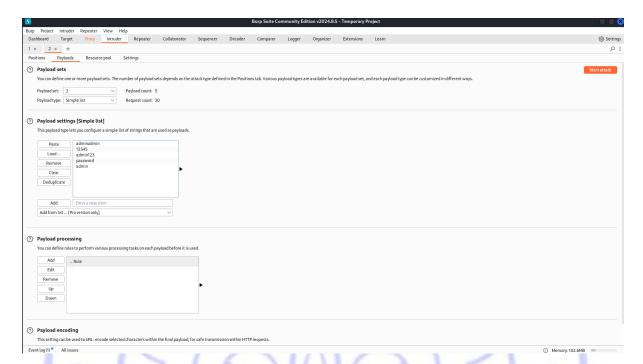


Now selecting the section where I do brute force.

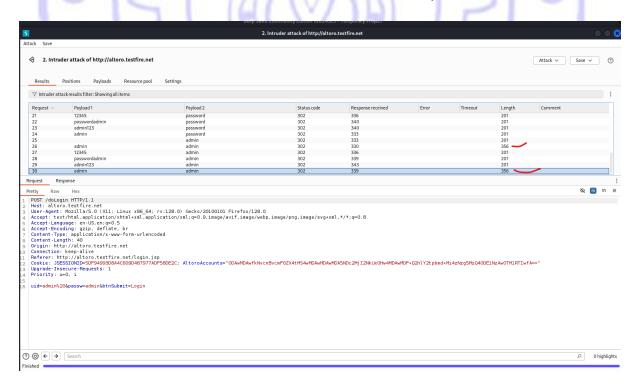




o Now, create a list which will be used in a brute force attack.

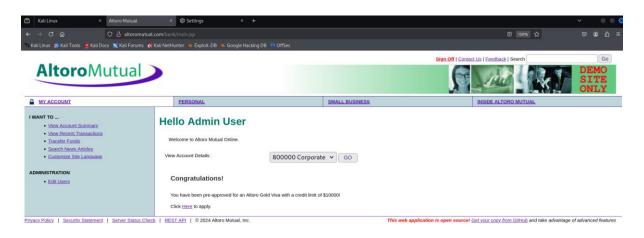


The attack find the username = "admin" and password = "admin".



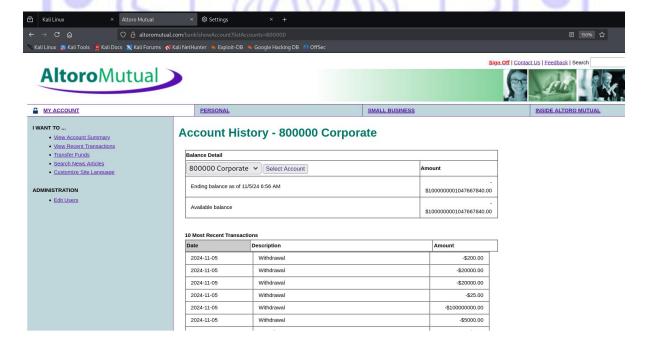


o Result -



The Brut force attack is successful.

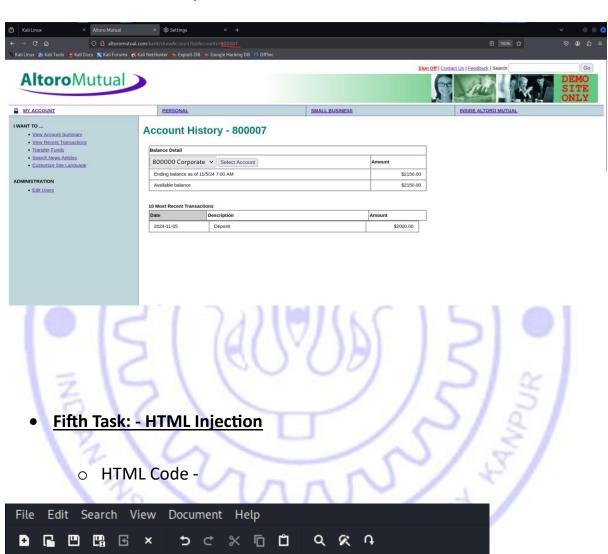
- Forth Task: Access Control Vulnerability
 - o If I log in to a website then I can see only my account details.





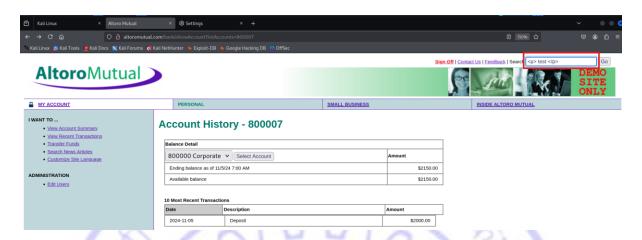
1 test

 But with some change in the parameter or URL, if I can see other account details, then it means its access control is broken.

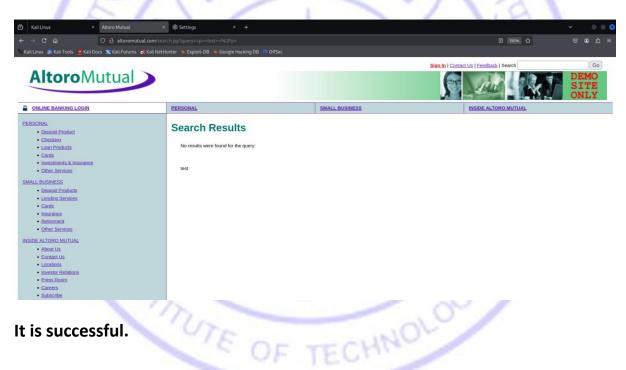




Paste this code in to search section.



Then the result comes.



It is successful.